UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MISSOURI

MARITZ HOLDINGS INC., Plaintiff, v. COGNIZANT TECHNOLOGY SOLUTIONS U.S. CORPORATION, Defendant.	Case No. 4:18-cv-00826-CDP

COGNIZANT'S MEMORANDUM OF LAW IN SUPPORT OF ITS MOTION TO DISMISS MARITZ' COMPLAINT FOR FAILURE TO STATE A CLAIM UPON WHICH RELIEF CAN BE GRANTED

Ronald J. Tenpas (admitted *pro hac vice*)
Patrick A. Harvey (admitted *pro hac vice*)
MORGAN, LEWIS & BOCKIUS LLP
1111 Pennsylvania Avenue, NW
Washington, DC 20004
Phone: (202) 739-3000
Fax: (202) 739-3001
ronald.tenpas@morganlewis.com
patrick.harvey@morganlewis.com

Jim Martin
DOWD BENNETT
7733 Forsyth Blvd
St. Louis, MO 63105
Phone: (314) 889-7300
Fax: (314) 863-2111
jmartin@dowdbennett.com

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

INTRODUCTION

This case relates to an alleged hacking and theft of gift cards from Plaintiff Maritz Holdings Inc. ("Maritz") after it fell victim to two phishing attacks in 2016 and 2017. But Maritz has not sued the perpetrator of those attacks. Instead, Maritz sued Cognizant Technology Solutions U.S. Corporation ("Cognizant"), a vendor of various IT services to Maritz, none of which are cybersecurity services. Maritz does not allege that Cognizant launched the cyberattacks or that Cognizant has a stash of stolen gift card information. Such a claim would be absurd on its face: Cognizant is a multinational S&P 500 and Fortune 200 corporation for which Maritz has been a valued client for nearly a decade.

Most of Maritz' Complaint is filler designed to hide the fundamental failures in its claims. Most tellingly, Maritz' Complaint describes the first phishing attack it allegedly suffered in 2016, but *does not contain a single allegation linking Cognizant to the attack.* The Complaint similarly fails to provide any specific facts directly linking Cognizant to the second cyberattack it allegedly suffered a year later in 2017. Instead, Maritz only alleges that "the attackers were accessing the Maritz system using accounts registered to Cognizant." ECF No. 1 ("Compl.") ¶ 43. In a world where user accounts can be compromised in myriad ways, where an earlier attack is alleged to have occurred and succeeded, and under statutory and pleading standards that require specific allegations of intent, this slender reed cannot come close to supporting Maritz' incredible claims.

Critically, Maritz does not (and cannot) allege facts suggesting that any Cognizant employee committed either the first or second attack; or even that any Cognizant employee committed some specific misconduct. Maritz also does not (and cannot) allege that it advised Cognizant of the first attack when it allegedly occurred in 2016; or the second attack when it allegedly occurred in 2017. Nor does Maritz set forth the forensic evidence linking responsibility for either attack to Cognizant, which was not responsible for Maritz' cybersecurity (a fact that presumably explains why Maritz never alerted Cognizant of these attacks until well afterward).

Those failures, as well as the others described below, make clear what is happening here. After having allegedly spent millions over more than two years to investigate its cyberattacks (*see id* ¶¶ 41–42), Maritz still has not provided Cognizant with any facts showing that Cognizant was responsible, despite repeated requests. In the absence of such facts, Maritz has filed this lawsuit alleging a mass of irrelevant pleading detail—detail that falls well short of necessary standards. As such, the entire Complaint should be dismissed with prejudice.

BACKGROUND

On January 1, 2010, Cognizant entered into a Master Services Agreement contract (the "MSA") with Maritz, agreeing to provide Maritz with various IT services. *Id.* ¶ 11; Compl. Ex. 1 § 4.1. While the MSA governs the overarching Maritz-Cognizant relationship, Cognizant received its actual work assignments through individualized "Statements of Work" ("SoWs"). MSA § 4.1. The parties entered into four different SoWs covering different portions of Maritz' business: (1) the Maritz Travel Company (Def. Ex. A), (2) MaritzCX (Def. Ex. B), (3) Maritz Motivation Solutions (Def. Ex. C), and (4) Maritz Enterprise Applications (Def. Ex. D).[1] None of the agreements provide for Cognizant to perform cybersecurity services, nor was cybersecurity ever part of the suite of services Cognizant provided to Maritz.

While the SoWs described different work scopes, they all provided a similar arrangement for Cognizant employees to access certain Maritz resources, such as Maritz databases and other Maritz systems. *See, e.g.*, Def. Ex. A at 3 ("Maritz will provide access/accounts/licenses to

[1] The SoWs are integral to the Complaint because they define the scope and nature of work Cognizant performed under the MSA. *See* MSA § 4.1. Consequently, the Court can consider them without converting the motion into one for summary judgment. *Ouwinga v. Benistar 419 Plan Servs., Inc.*, 694 F.3d 783, 797 (6th Cir. 2012).

appropriate systems, databases, tools, repositories and user access rights to Cognizant associates to perform the activities in scope."). For work to be performed at Maritz locations, Maritz provided the hardware for Cognizant employees. *Id.* at 4. For work to be performed offshore or elsewhere, Maritz was responsible for "identify[ing] a secure method for Cognizant to connect to Maritz resources for necessary work streams." *Id.* In other words, Maritz was itself master of the access rights and protocols that controlled Cognizant employee access to Maritz' IT systems.

In 2016, Maritz allegedly fell victim to a phishing attack that caused it over $11 million in losses. *See* Compl. ¶¶ 18–36. The attack was launched by unknown perpetrators and did not involve Cognizant in any way. *See id.* In February and March 2017, Maritz apparently suffered a second, smaller attack. *Id.* ¶ 37. The unidentified perpetrators allegedly sent phishing e-mails containing a URL that, when accessed, placed "remote access tools" on Maritz' computer systems that allowed the perpetrators to use co-opted accounts to steal confidential information from Maritz' servers. *Id.* ¶ 39. Maritz alleges that, later, in "April 2017, someone using a Cognizant account utilized the 'fiddler' hacking program to circumvent cyber protections that Maritz had installed several weeks earlier." *Id.* ¶ 43. Notably, Maritz does not identify the specific Cognizant account and does not allege that the employee associated with that account (or anyone at Cognizant) actually was the party using the Cognizant account or was aware of the recently installed cybersecurity protocols.

Maritz also does not allege that Cognizant either encouraged, directed, or was even aware of the hacking when it occurred. To the contrary, Maritz did not tell Cognizant about these attacks until much later. Still, Maritz alleges that "Cognizant was *negligent or reckless*" in allowing "one or more of its employees and/or third parties to intentionally access Maritz' network as described herein." *Id.* ¶ 51. Similarly, based "on information or belief," rather than alleging specifically that

Cognizant condoned specific activity, with supporting facts, Maritz instead alleges only that "one or more of Cognizant's employees, while acting in the scope of their employment and under the control and supervision of Cognizant, intentionally accessed Maritz'[] network and removed or copied confidential information belonging to Maritz . . . without authorization and/or by exceeding their authorization" *Id.* ¶¶ 50, 60. In other words, Maritz relies on notions of vicarious liability for its tort and statutory claims.

ARGUMENT

When evaluating a motion to dismiss, courts are required to "assume the truth of the facts alleged." *Dahlen v. Shelter House*, 598 F.3d 1007, 1010 (8th Cir. 2010). But facts in the complaint must be alleged with a reasonable level of particularity—the court may not consider bald assertions or conclusory statements. *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). A valid complaint "must contain enough factual allegations, accepted as true, to state a claim for relief that is 'plausible on its face.'" *Process Controls Int'l, Inc. v. Emerson Process Mgmt.*, 753 F. Supp. 2d 912, 919 (E.D. Mo. 2010) (quoting *Iqbal*, 556 U.S. at 678). "If a complaint pleads facts that are *merely consistent with* defendant's liability, it stops short of the line between possibility and plausibility of entitlement to relief and should be dismissed for failure to state a claim." *Id.* (emphasis added) (citation omitted).

I. Maritz Does Not Allege That Cognizant Was Involved with the 2016 Attack.

The Complaint makes no allegations connecting Cognizant in any way with the larger 2016 attack, and includes no factual allegations at all related to the cause of that attack. That is a glaring and fatal omission, confirming that Maritz has sued Cognizant in order to point the finger at someone else for its own cybersecurity failings. Those allegations should thus be disregarded.

II. Maritz’ Statutory Claims Fail Because It Does Not Allege That Cognizant Acted Intentionally.

Maritz asserts claims under the federal Computer Fraud and Abuse Act (“CFAA”) and the Missouri Computer Tampering Statutes (“MCTS”). The statutes are similar. Both statutes are primarily criminal, but also incorporate a potential civil action for victims of certain computer crimes. *See* 18 U.S.C. § 1030(g); MO. ANN. STAT. § 537.525.1. Unsurprising for statutes primarily designed to prevent criminal conduct, both require proof that a defendant acted with specific criminal intent before liability can be found. 18 U.S.C. § 1030(a)(2) (“Whoever . . . *intentionally* accesses a computer without authorization or exceeds authorized access” (emphasis added)); MO. ANN. STAT. § 569.095 (“A person commits the crime of tampering with computer data if he *knowingly* and without authorization . . . .” (emphasis added)).

For a complaint addressing a criminal scheme involving the theft of millions of dollars, the absence of one allegation in the Maritz Complaint sticks out: Maritz does not allege (conclusorily or otherwise) that Cognizant intentionally hacked Maritz’ computer systems. Instead, Maritz invokes vicarious liability, alleging that Cognizant was “negligent or reckless” in supervising its employees (Compl. ¶ 51), and that an unnamed Cognizant employee (or employees—Maritz doesn’t know and doesn’t specify) intentionally hacked Maritz computer systems to steal gift cards while acting in the scope of their Cognizant employment (*id.* ¶ 50). Such pleading is insufficient for two independent reasons. First, Maritz fails to plead facts to even support an inference that any Cognizant employee acted intentionally to cause the attacks. Second, regardless of any Cognizant employee’s conduct, the Complaint makes no claim that Cognizant directed, encouraged, or profited from its employee’s misconduct.

A. Maritz' Complaint Does Not Plausibly Allege That Any Cognizant Employee Hacked Into Maritz' System.

To hold Cognizant liable for the misdeeds of its employees, Maritz must first plausibly allege that Cognizant's employees engaged in wrongdoing. *See Crawford v. Signet Bank*, 179 F.3d 926, 928 (D.C. Cir. 1999); Dan B. Dobbs et al., *The Law of Torts* § 425 n.15 (2d ed.). But Maritz' computer tampering claims fail for this elementary reason: the Complaint does not plausibly allege that any Cognizant employee—let alone Cognizant as a whole—engaged in any hacking and theft of valuable gift card information.

Maritz does not allege that Cognizant was involved with the 2016 attack. For the 2017 attack only, Maritz alleges that "attackers were accessing the Maritz systems using accounts registered to Cognizant." Compl. ¶ 43. But the nature of the attack is important. According to Maritz, successful "[s]pear phishing or 'targeted emails'" were directed to Maritz accounts, phishing emails caused "remote access tools" to be placed on Maritz' computer systems, and those tools allowed "perpetrator(s) to access[] Maritz'[] systems to obtain confidential information." Compl. ¶ 39. "Phishing involves an attempt to acquire information such as usernames, passwords, or financial data by a perpetrator masquerading as a legitimate enterprise." *Choice Escrow & Land Title, LLC v. BancorpSouth Bank*, 754 F.3d 611, 615 (8th Cir. 2014). By definition, employees or accounts that fall victim to phishing attacks are not in cahoots with the hacker—they're the marks. Thus, alleging that a Cognizant account was associated with a phishing attack does not mean a Cognizant employee was behind it, and in fact suggests the opposite. This cannot be cured through Maritz' conclusory statements that Cognizant employees acted "intentionally" (Compl. ¶¶ 50, 60) because conclusory allegations about intent are disregarded. *See, e.g.*, *Thomas v. Zion Lutheran Sch.*, No. 4:12CV2243 JCH, 2012 WL 6093704, at *3 (E.D. Mo. Dec. 7, 2012) (disregarding "conclusory allegations and assumptions as to defendants' states of mind").

Although Maritz must include specific facts to make it not just "conceivable" but "plausible" that Cognizant employees used their accounts to *intentionally* access the gift card information, *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007), its Complaint lacks such allegations. Maritz does not allege that Cognizant employees sent the phishing emails. It does not allege Cognizant employees cooperated with or assisted the cyberattacks. And it does not identify any employee who allegedly committed the crime. Moreover, the Complaint acknowledges the success of the phishing attacks, making it likely that any account compromise resulted from those attacks, not from the accounts being used by authorized users. That makes it even more unreasonable to infer that Cognizant employees acted intentionally to cause the hacks. *See Hiland Dairy, Inc. v. Kroger Co.*, 402 F.2d 968, 973 (8th Cir. 1968) (court cannot make "unreasonable inferences or unwarranted deductions of fact" when ruling on a motion to dismiss).

B. Maritz' Statutory Claims Fail Because It Does Not Allege That Cognizant Directed the Hacking.

For Cognizant to be vicariously liable, it is not sufficient to allege that its employees violated the CFAA or MCTS. Instead, Maritz must allege, at an absolute minimum, that Cognizant affirmatively "urged," "induced," "encouraged," or "directed" the wrongful conduct for its own benefit to trigger vicarious liability.[2] Indeed, one court has concluded that vicarious liability claims are never permissible under the CFAA.[3]

[2] *See, e.g.*, *Butera & Andrews v. Int'l Bus. Machines Corp.*, 456 F. Supp. 2d 104, 112 (D.D.C. 2006) ("urged"); *Agilysys, Inc. v. Hall*, 258 F. Supp. 3d 1331, 1343–44 (N.D. Ga. 2017) ("directed" or "induced"); *Schlumberger Tech. Corp. v. McReynolds*, No. 15-2455, 2016 WL 4597627, at *5 (W.D. La. Sept. 1, 2016) ("urged" or "encouraged"); *Charles Schwab & Co. v. Carter*, No. 04-7071, 2005 WL 2369815 (N.D. Ill. Sept. 27, 2005) ("urged"); *Garland-Sash v. Lewis*, No. 05 CIV. 6827 (WHP), 2007 WL 935013, at *4 (S.D.N.Y. Mar. 26, 2007), *aff'd in part, vacated in part*, 348 F. App'x 639 (2d Cir. 2009) ("directed").

[3] *Doe v. Dartmouth-Hitchcock Med. Ctr.*, 2001 WL 873063, at *6 (D.N.H. July 19, 2001) ("Expanding the private cause of action created by Congress to include one for vicarious liability against persons who did not act with criminal intent . . . would be entirely inconsistent with the plain language of the statute.").

The *Butera & Andrews* case illuminates the scienter requirement well, and is indistinguishable from the case at bar. In that case, the plaintiff fell victim to a cyberattack. *Butera & Andrews*, 456 F. Supp. 2d at 107. After a forensic investigation, it concluded that the attack originated from an IBM facility. *Id.* The plaintiff then filed suit against IBM and an unnamed John Doe employee, alleging violations of the CFAA and asserting direct and vicarious theories of liability. *Id.* As with the instant Complaint, the plaintiff "[did] not allege that [the defendant-employer] orchestrated, authorized, or was otherwise aware of [the] attacks. *Id.* at 109. Rather, the plaintiff claimed "'upon information and belief' that [the unnamed defendant], in his capacity as IBM employee or agent, initiated, directed and managed" the attacks. *Id.* In the face of those limited allegations, the court dismissed the CFAA claim against IBM because plaintiff failed to plead facts demonstrating that IBM "tacitly knew and approved of the conduct allegedly engaged in by its employees or agents." *Id.* at 113.

So too here. Maritz has not included even a conclusory allegation that Cognizant directed or profited from the attack, much less provided specific facts to support such an allegation. At best, Maritz' theory of liability is that Cognizant negligently or recklessly failed to prevent its employees from stealing the gift cards. Compl. ¶ 51. No court has found an employer vicariously liable under the CFAA or MCTS based on scant allegations of negligent, or even reckless, employee supervision. Holding otherwise would be particularly dramatic given that it would also mean that companies would become *criminally liable* for the unsanctioned actions of their subordinates. *See United States v. Thompson/Center Arms Co.*, 504 U.S. 505, 518 n.10 (1992) (indicating that statute with criminal and civil applications should be interpreted the same way in civil and criminal contexts).

Maritz' affirmative allegations of "negligence" and "recklessness" are thus self-defeating. Negligent and even reckless supervision cannot trigger CFAA or MCTS liability. And because an employer cannot simultaneously negligently or recklessly supervise its employees while also directing the employee to engage in misconduct, the current allegations fatally undercut any future claim that Cognizant directed or profited from an employee's misconduct. Thus, Maritz' statutory claims should be dismissed with prejudice.

III. Maritz Fails to State a Claim for Conversion.

Conversion is a claim that a defendant *intentionally* took a plaintiff's property and deprived the plaintiff's rights to that property. *See AIG Agency, Inc. v. Missouri Gen. Ins. Agency, Inc.*, 474 S.W.3d 222, 228-29 (Mo. Ct. App. 2015). Lacking allegations of specific intent, Maritz' conversion claim therefore suffers from the same infirmaries as its statutory claims. *See supra* § II. Nor does Maritz even allege that Cognizant took its property.

Vicarious liability principles do not change the outcome. Maritz does not plausibly allege that any Cognizant employee intentionally took Maritz's gift cards. Under Missouri law, moreover, Cognizant cannot be held vicariously liable for the torts of its employees unless the torts were committed within the "course and scope of their employment." *Inman v. Dominguez*, 371 S.W.3d 921, 924 (Mo. Ct. App. 2012). The idea that Cognizant employees were acting within the scope of their employment by allegedly stealing gift cards cannot be taken seriously and, indeed, is not alleged here with any plausible support.[4] Hacking computers to acquire gift cards is not what Cognizant, a company named as one of Fortune's most admired companies ten years in a row, asks its employees to do. *Cf.* Compl. ¶ 4 (Cognizant is "one of the world's leading providers

[4] Like all conclusory allegations, a mere assertion in the Complaint that Cognizant employees were acting within the scope of their employment is insufficient. *See, e.g.*, *Oetting v. Heffler, Radetich & Saitta, LLP*, No. 11-253, 2011 WL 3055235, at *3 (E.D. Mo. July 25, 2011).

of information technology, consulting, and business process outsourcing services."). The alleged criminal activity lacks any hallmarks of an employee serving its employer. Hacking and stealing from clients does not "further the business or interests" of Cognizant, nor does Maritz claim it would. *Inman*, 371 S.W.3d at 924 (Mo. Ct. App. 2012). Nor do those crimes "naturally arise from the performance" of Cognizant's work to provide IT consulting services to Maritz. *Id.*; *see also* MSA. And there is no claim that the gift cards ended up in Cognizant's corporate control. If rogue Cognizant employees perpetuated the hacking and theft (and there is no plausible allegation that they did) they were doing so "entirely for [their] own purposes" and "there can be no *respondeat superior* liability." *Doe by Doe v. B.P.S. Guard Servs., Inc.*, 945 F.2d 1422, 1425 (8th Cir. 1991).

Maritz' conclusory allegation of inadequate supervision also cannot rope Cognizant into liability for an employee's conversion. *See* Compl. ¶¶ 51, 58. For example, to be liable for conversion based on negligent hiring, Maritz must plead facts to support an independent claim for negligent hiring. *See* Restatement (Third) of Agency § 7.05 cmt. c (2006). Similarly, Maritz must allege (1) that Cognizant "knew or should have known of the employee's dangerous proclivities," (i.e., that Cognizant knew that it hired employees with a history of hacking and stealing), and (2) that Cognizant's negligence in hiring that employee "was the proximate cause of the plaintiff's injuries." *Gibson v. Brewer*, 952 S.W.2d 239, 246 (Mo. 1997). Maritz does not even *identify* the employee(s) who committed the alleged conversion, let alone allege that Maritz should have known they had a record of computer fraud or theft. Maritz fails to state a claim for conversion.

IV. Maritz Fails to State a Claim for Breach of Contract.

Without tying specific breaches to particular MSA provisions, Maritz claims Cognizant breached the MSA in four different ways:

- Cognizant failed to prevent its employees or other unauthorized personnel from accessing Maritz' systems for improper purposes. Compl. ¶ 64.

- Cognizant failed to prevent its employees from sharing credentials and usernames for Cognizant accounts in violation of industry standards and Maritz' company policy. *Id.*

- Cognizant failed to take responsibility for the above-referenced security breaches. *Id.*

- Cognizant billed Maritz for time spent by Cognizant's employees when they were accessing Maritz' computer systems for improper purposes. *Id.* ¶¶ 66–70.

Each theory fails to state a valid claim for breach of contract.

A. Cognizant Did Not Promise That It Would Prevent Maritz' Computer Data from Being Accessed for Improper Purposes.

Maritz does not identify a contractual provision where Cognizant allegedly promised to "prevent Cognizant employees or other unauthorized personnel from accessing Maritz'[] systems for improper purposes." There's a reason: No such provision exists. Cognizant was not hired to protect Maritz' computer network and therefore would never warrant or guarantee that it would never get hacked. Nor can such a promise be inferred from the MSA. Cognizant made a variety of representations and warranties in the MSA—but a cybersecurity guarantee was not one of them. MSA §§ 13.1–13.2. And lest there be any doubt, Cognizant explicitly disclaimed any representations, warranties, or conditions not expressly included in the contract. MSA § 14.1. Cognizant cannot break a promise it never made, and Maritz cannot sue on a nonexistent promise. *See Mw. Printing, Inc. v. AM Int'l, Inc.*, 108 F.3d 168, 171 (8th Cir. 1997).

B. Even if Cognizant Employees Shared Credentials, That Does Not Support a Breach of Contract Claim Based on Hacking.

The Complaint's second theory is that Cognizant breached its contract by failing to prevent its employees from sharing credentials and usernames for Cognizant accounts *with themselves*, in violation of industry standards and Maritz policy. Compl. ¶ 64. Maritz cites no specific contract provision to support the claim, and only one contractual provision even arguably speaks to this. MSA Section 9.1 states in part that the parties mutually agree that Cognizant will use "at least the same degree of care as it uses to avoid unauthorized use, disclosure, or dissemination of its own Confidential Information of a similar nature, but not less than reasonable care."

The Complaint, however, fails to allege any facts regarding how Cognizant handles its own "confidential information of a similar nature." Even if it had, such an allegation would be implausible because sharing credentials *among* Cognizant employees does not result in releasing confidential information to unauthorized individuals outside Cognizant. Maritz does not allege that external sharing occurred.

Even assuming that Cognizant had a contractual obligation for its employees not to share credentials internally, Maritz' theory of breach still fails. To state a valid claim for breach of contract, Maritz must allege damages that stem *from the breach*—not from unrelated actions or contract provisions. *See Guidry v. Charter Commc'ns, Inc.*, 269 S.W.3d 520, 533 (Mo. Ct. App. 2008) (recognizing that "damages . . . are only those which are incidental to, and directly caused by, the breach"). Maritz does not allege that the internal sharing of login credentials caused Maritz' injuries and does not link the alleged credential sharing to the attack. Nor would any allegation make sense. An external phishing attack—which Maritz alleges is the source of its injuries—succeeds or fails regardless of the internal sharing of passwords: the hacker launches a phishing attack because he lacks access with a password. Thus, the alleged sharing of passwords cannot be the basis of a viable breach of contract claim because there is no stated link between that and the asserted damages.

C. The Contract Does Not Contain an Obligation for Cognizant to "Take Responsibility" for Any Breaches.

The Complaint's third theory is that Cognizant breached the contract by failing "to take responsibility for the security breaches." Compl. ¶ 64. It is not clear what Maritz means by "take responsibility," since Maritz did not even notify Cognizant of the first or second attacks until well after both had occurred. Perhaps Maritz means to say that Cognizant is obligated to indemnify Maritz for any losses Maritz suffered from the cyber-attack. That claim, however, is foreclosed because Cognizant never promised to indemnify Maritz for losses stemming from a security breach (MSA §§ 11.1–11.1.4), and Cognizant explicitly disclaimed indemnifying Maritz for any losses other than those the agreement explicitly included (MSA § 14.2).

D. Conclusory Allegations That Cognizant Employees Billed for Time Spent Engaging in Cyberattacks Cannot Support a Breach of Contract Claim.

Maritz' final theory is that Cognizant breached the MSA by billing Maritz for service time that was actually spent "engaging in attacking Maritz'[] system rather than providing the services Cognizant contracted to provide." Compl. ¶ 67. This theory fails for at least three reasons.

First, this theory of breach is based on the premise that Cognizant employees contributed to the cyberattack. But, as explained above, the Complaint does not adequately allege that any employees engaged in wrongdoing. Accordingly, this theory of breach fails for the same reason as the CFAA, MCTS, and conversion claims. *See supra* § II.A.

Second, the theory is utterly devoid of detail. In particular, the Complaint fails to identify (1) which employees allegedly billed time improperly (2) under which SoW (3) for what amounts, or even (4) what provision of the contract such billing violates. Maritz must plead facts sufficient to provide Cognizant "fair notice of what the plaintiff's claim is and the grounds upon which it rests." *Swierkiewicz v. Sorema N.A.*, 534 U.S. 506, 514 (2002). Maritz' sparse pleading leaves Cognizant in the dark and is therefore insufficient.

Third, even if Maritz plausibly alleged Cognizant employee malfeasance, and even if it alleged that an employee improperly billed his time to Maritz' account, Maritz still fails to allege facts sufficient to show that any improper charges were actually billed to or paid by Maritz. Each of Cognizant's projects was billed at a *fixed monthly rate* rather than by the hour. *See* Def. Exs.

A–D §§ 6(e) & 8. Thus, it is implausible that billing time "to the account" could occur in any fashion that increased Maritz' costs or enriched Cognizant. The Complaint's failure to identify a SoW, or to allege that improper time was billed to a pay-by-the-hour project, means the Complaint fails to allege any damages associated with this theory of breach.

V. Maritz Fails to State a Claim for Negligence.

In order to prevail on a negligence claim, a plaintiff must plead and prove that the defendant had a duty, that the defendant breached the duty, that the breach proximately caused an injury, and damages. *G.E.T. ex rel. T.T. v. Barron*, 4 S.W.3d 622, 624 (Mo. Ct. App. 1999). The Complaint fails to identify any legally cognizable duty that Cognizant breached.

The Complaint identifies two duties that Cognizant purportedly owed to Maritz: "a duty to prevent foreseeable harm to Maritz, including taking reasonable safeguards to prevent its employees and third parties from using Cognizant accounts to hack Maritz'[] computer network," Compl. ¶ 72, and "a duty to safeguard the credentials and usernames issued to Cognizant employees with access to Maritz'[] system," *id.* ¶ 73. But there is no general tort duty to protect another's computer network, nor is there a general duty to safeguard login credentials another has issued. Rather, these purported duties arose solely from the MSA. *Compare* Compl. ¶¶ 72-73 *with id.* ¶ 64. That serves as an insurmountable obstacle for Maritz' negligence claim. Maritz cannot take a bargained-for set of contractual duties and transmute them to generalized tort duties. As explained above, the bargained-for contractual duties are limited and have not been fairly alleged to have been breached, but even if they were, "[u]nder Missouri law, a breach of contract alone does not give[] rise to a tort." *Pippin v. Hill-Rom Co.*, 615 F.3d 886, 889 (8th Cir. 2010). That is, "[t]he mere failure to perform a contract cannot serve as the basis of tort liability for negligence." *State ex rel. William Ranni Assoc., Inc. v. Hartenbach*, 742 S.W.2d 134, 140 (Mo.

1987) (en banc). Accordingly, Maritz' negligence claim must fail for lack of a legally cognizable duty that exists outside the contract.[5]

VI. Maritz Fails to State a Claim for Unjust Enrichment

Maritz' claim for unjust enrichment based on allegations that Cognizant billed Maritz for the time that unknown Cognizant employees supposedly spent hacking into Maritz' network fails as a matter of law for the same reasons its analogous breach of contract claim does. *See supra* § IV.D. In addition, under Missouri law, a plaintiff cannot recover under both unjust enrichment and breach of contract. *Affordable Communities of Mo. v. Fed. Nat. Mortg. Ass'n*, 714 F.3d 1069, 1077 (8th Cir. 2013). While Maritz claims that it is pleading unjust enrichment in the alternative to its contract claim, it incorporates its breach of contract allegations into the claim. *See* Compl. ¶ 76 (incorporating allegations 1–75), *id.* ¶¶ 8–17 (describing the contract terms); *id.* ¶¶ 61–70 (alleging that Cognizant breached the MSA). That is improper. "A party cannot properly plead a valid quasi-contract theory by including allegations to support the claim that indicate that the parties' relationship was governed by an express agreement." *Marks v. Compo Steel Prod., Inc.*, No. 08C5049, 2008 WL 5221172, at *4 (N.D. Ill. Dec. 12, 2008).[6]

CONCLUSION

For the foregoing reasons, Cognizant respectfully requests that the Court dismiss the Complaint with prejudice.

[5] Maritz' claim that Cognizant also negligently failed to hire and train employees fails for the same reasons stated in Section III above.

[6] Insofar as Maritz seeks to bring a separate claim for equitable accounting, Maritz does not include any of the four elements needed to support its claim. *Shaner v. Sys. Integrators, Inc.*, 63 S.W.3d 674, 677 (Mo. Ct. App. 2001) ("Four elements are required to establish equitable jurisdiction for an accounting: the need for discovery, the complicated nature of the accounts, the existence of a fiduciary or trust relationship and the inadequacy of legal remedies."). To the degree such a claim is pled, it should therefore also be dismissed.

Dated: September 4, 2018

Respectfully submitted,

/s/ Ronald J. Tenpas
Ronald J. Tenpas*
Patrick A. Harvey*
MORGAN, LEWIS & BOCKIUS LLP
1111 Pennsylvania Avenue, N.W.
Washington, DC 20004
Phone: (202) 739-3000
Fax: (202) 739-3001
E-mail: ronald.tenpas@morganlewis.com
patrick.harvey@morganlewis.com

*admitted *pro hac vice*

-and-

Jim Martin
DOWD BENNETT LLP
7733 Forsyth Blvd.
St. Louis, MO 63105
Phone: (314) 889-7300
Fax: (314) 863-2111
Email: jmartin@dowdbennett.com

Counsel for Defendant Cognizant Technology Solutions U.S. Corporation

CERTIFICATE OF SERVICE

I certify that on September 4, 2018, a true copy of the foregoing was served by the ECF e-filing system on the following:

Brian A. Lamping
blamping@thompsoncoburn.com
Jan P. Miller
jmiller@thompsoncoburn.com
Kristen E. Sanocki
ksanocki@thompsoncoburn.com
Thompson Coburn, LLP
One US Bank Plaza
505 N. 7th Street
St. Louis, MO 63101

I further certify that true and correct copies of Exhibits A-D were served on opposing counsel via e-mail pursuant to written agreement, as Cognizant is filing a motion seeking leave to file the exhibits under seal.

/s/ *Ronald J. Tenpas*
Ronald J. Tenpas